



*National
Security
Agency*

DoD Bridge Certification Authority Technology Demonstration

Lessons Learned - Future Plans

Federal Public Key Infrastructure Technical Working Group
5 April 2000

Dave Fillingham, NSA
dwfilli@missi.ncsc.mil

Overview

- Phase I
 - Goals
 - Implementation
 - Results
 - Lessons Learned
- Phase II
 - Goals
 - Implementation
- Summary

Phase I - Goals

- Demonstrate the feasibility of the BCA concept
 - Implement a bridged PKI containing both hierarchical and mesh PKIs, based on existing or slightly modified CA products
 - Demonstrate the ability of messaging clients to successfully exchange and process digitally signed traffic using the Bridge CA

Phase I - Goals

- Demonstrate the Border Directory concept
- Develop reference implementation software
 - certificate path development
 - processing certificate path processing
 - Make this software freely available to accelerate application developments
 - Demonstrate the use of this software via integration into e-mail clients implementing S/MIME V3 clients

Phase I - Implementation

- Approximately ten month effort
 - March - December 1999
 - Formal presentations started January 2000
- Nine Vendors worked as one team
 - Three CA vendors
 - Two Systems Engineering/Tech Support vendors
 - Two software development vendors
 - One directory vendor
 - One messaging application vendor

Phase I - Systems Engineering

- A&N Associates

- Project Planning and Management
- Overall Systems Engineering
- Technical Interoperability Profile Development
- Scenario Development
- Final Report Development

- Booz-Allen and Hamilton

- Certificate and CRL Development

Phase I - Infrastructure Components

- Motorola
 - Modified NSM/MISSI Certification Authority Workstation
- SPYRUS
 - S²CA
 - Provided SPYRUS Cards (Cryptographic Engine, Token)
- Entrust Technologies
 - Four CA mesh PKI
 - Four associated directory system agents
 - Entrust PKI toolkit
- Chromatix (Entegrity)
 - Directory System Agents
 - Directory expertise

Phase I - Software Development

■ J.G. Van Dyke and Associates

- Developed Certificate Management Library (CML)
- Developed S/MIME Freeware Library (SFL)
- Tested/Integrated demonstration in laboratory
- Provided demonstration facilities

■ CygnaCom Solutions

- Developed Certificate Path Development Library (CPDL)
- Integrated CPDL, CML, SFL into Eudora Client
- Integrated Entrust Toolkit into Eudora Client (on behalf of Entrust)
- Tested/Integrated demonstration in laboratory
- Provided demonstration facilities

Phase I - Client Development

■ Raytheon

- Developed BCA enabled S/MIME E-Mail Client based on Novell Groupwise, SFL, CML, CPDL

Phase I - Technical Interoperability Profile

- IETF LDAP V2 Directory Schema
- RSA/MD5 Signatures
- S/MIME V3 Application Layer Security Protocol
- X.500 Directory Systems Protocol Chaining
- X.509 Certificates and Revocation Lists

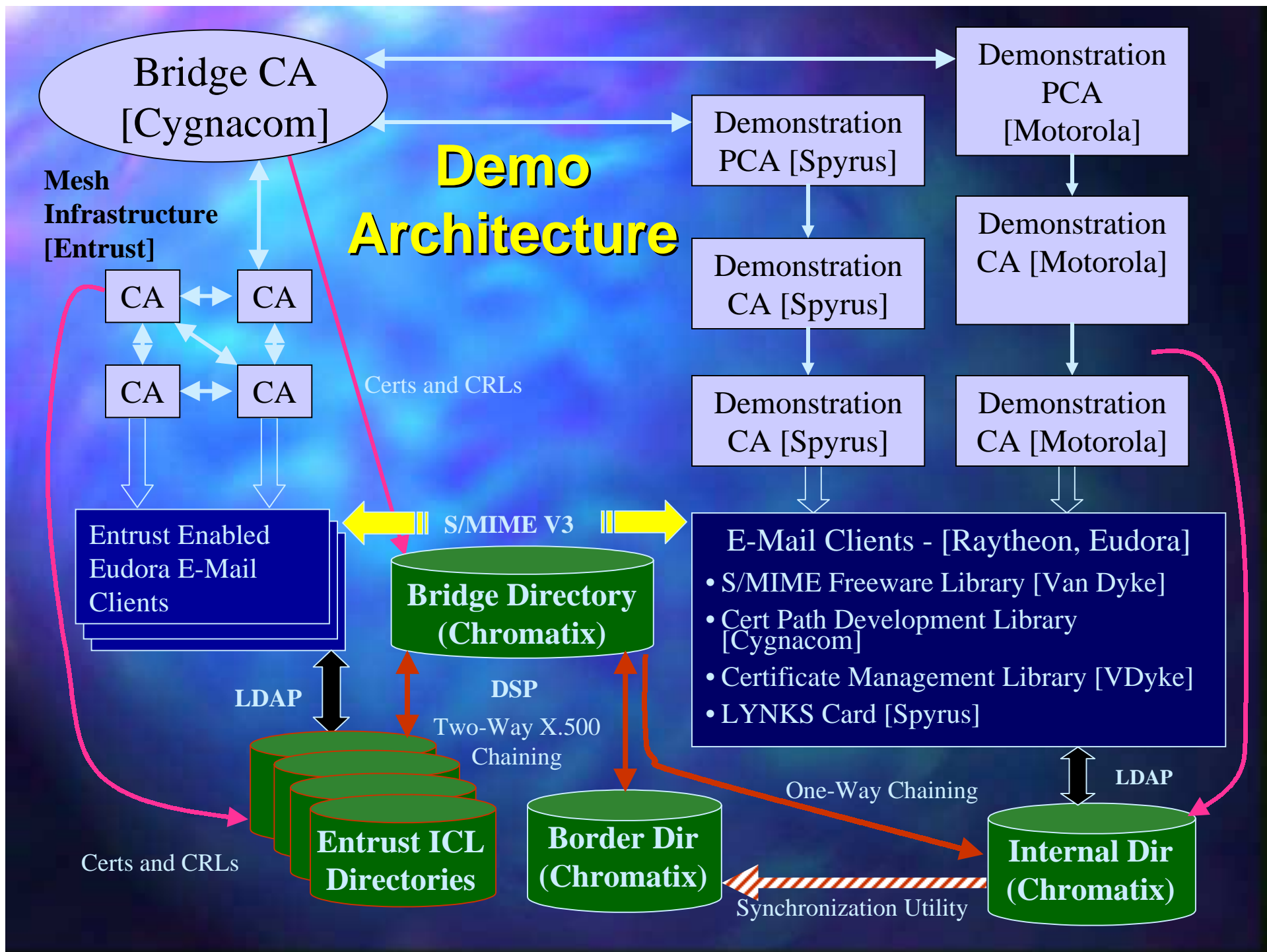
Available Software Modules

- Certificate Path Development Library
 - Developed by Cygnacom
- Certificate Management Library
 - Developed by J.G. Van Dyke and Associates
- S/MIME Freeware Library
 - Developed by J.G. Van Dyke and Associates

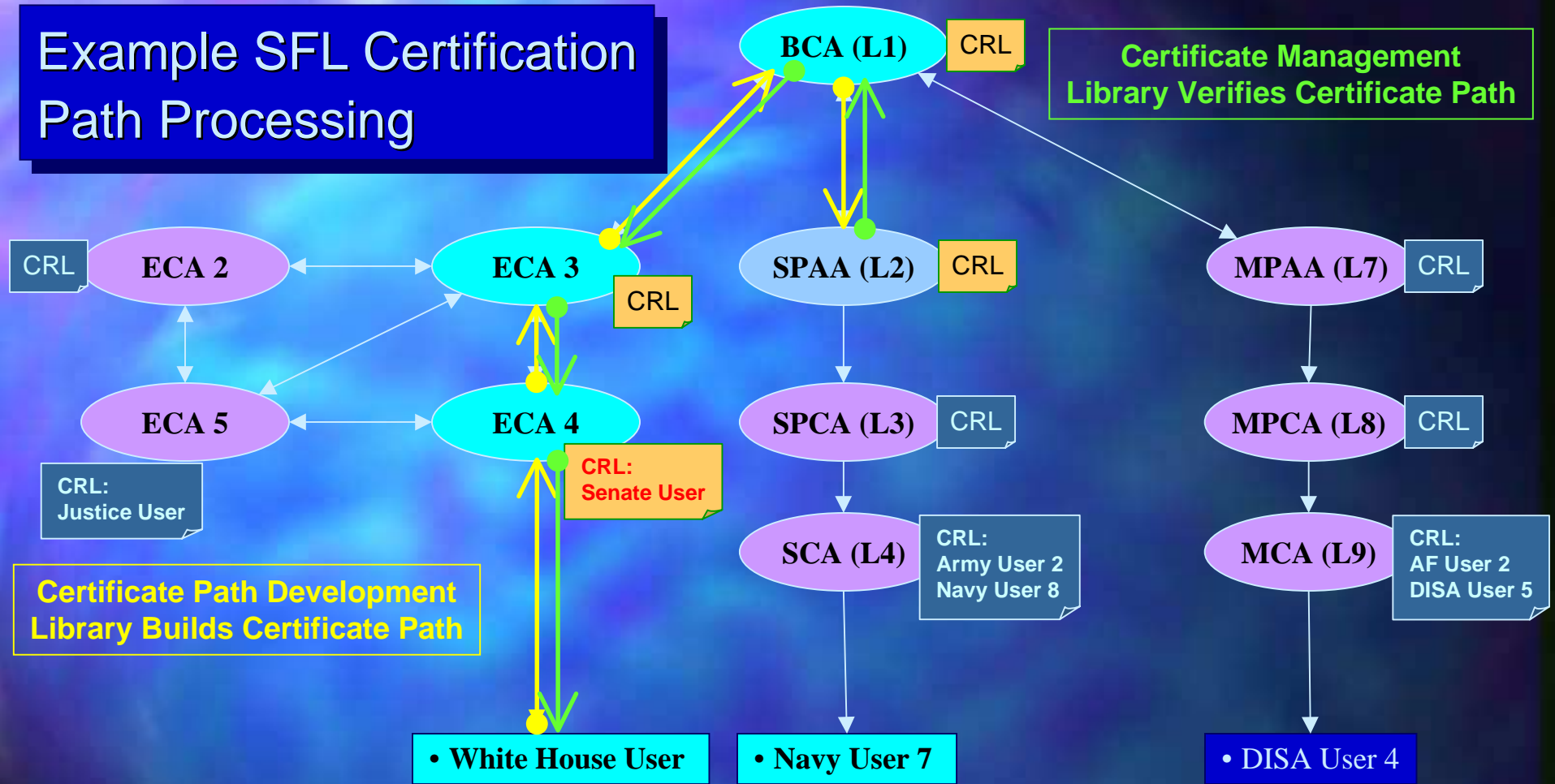


Free Software

- Certificate Path Development Library
 - <http://www.cygnacom.com/cpl/>
- Certificate Management Library
 - <http://www.armadillo.huntsville.al.us/software/certmgmt/index.html>
- S/MIME Freeware Library
 - <http://www.armadillo.huntsville.al.us/software/smime/index.html>



Example SFL Certification Path Processing

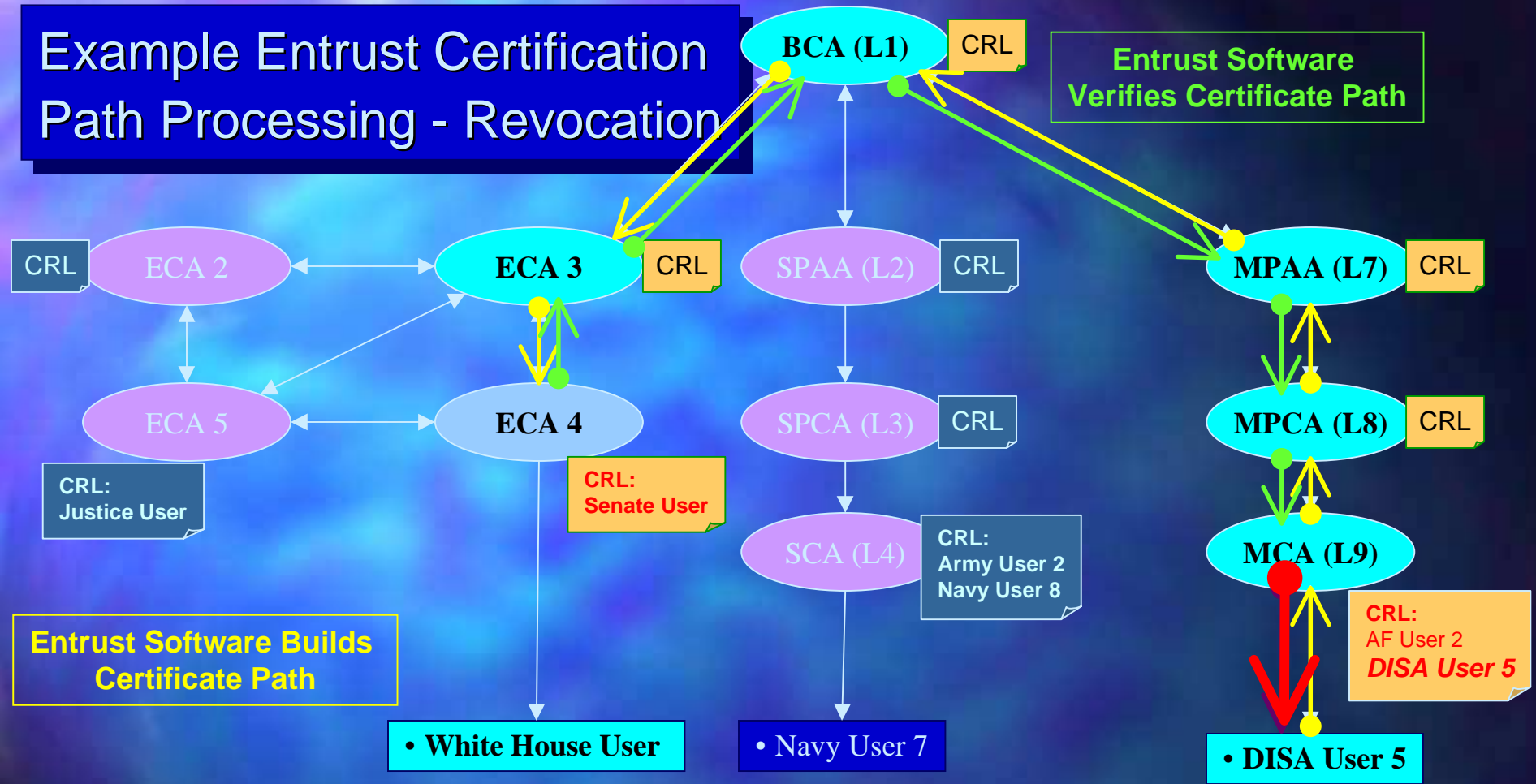


Entrust User
Sends Signed
Message to
SPYRUS
User



SPYRUS User
Builds and Verifies
Path from SPAA to
White House
(Entrust) User
Through BCA

Example Entrust Certification Path Processing - Revocation



Entrust User **Builds** and **Verifies** Path from own CA to AF User Through BCA

~~Signed Message, Signature Rejected!~~

Revoked
Motorola User Sends Signed Message to entrust User

Phase I - Results

- BCA concept works - at least in the lab!
 - Mix of mesh and hierarchical PKIs
 - Four different CA products
- Certificate paths are successfully built
 - Entrust toolkit
 - Certificate Path Development Library
- Certificate paths are successfully verified
- Directory chaining among Border Directories can be basis of directory interoperoperation

Phase I - Lessons Learned

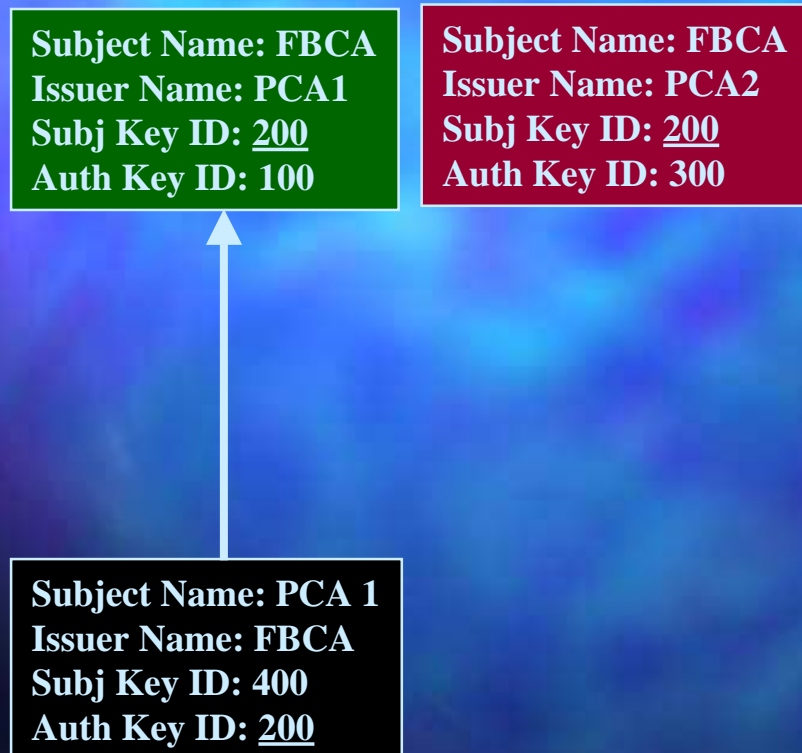
- Ease of integrating required certificate processing functions varied greatly based on application architecture
- Directory interoperation can be difficult
 - Difficult - but so far, always doable
 - Cross-vendor chaining requires careful directory configuration
 - Latent standards implementation errors can surface during cross-vendor directory integration

Phase I - Lessons Learned

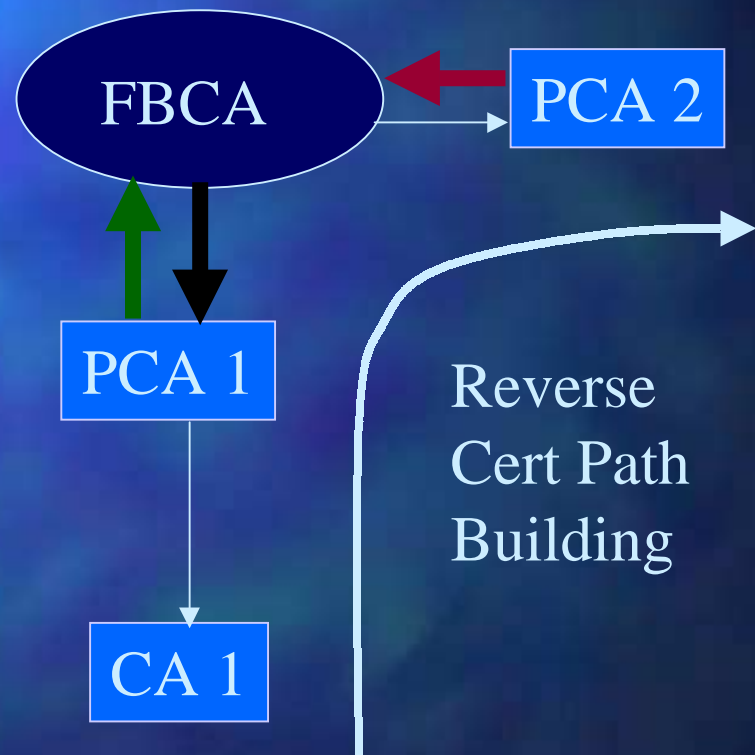
- Dominant performance factor: Directory lookups
 - Approximate signature verification times “first time” (without caching) 5 - 10 seconds
 - Once certificate path is cached - about 1 second
 - Vast majority of signature verifications will use cached chains
- Common error: setting path length constraints to 1 or 0
- Authority Key Identifier - Useful extension, but if clients built based on a specific infrastructure's implementation, problems result

Phase I - Lessons Learned - Authority Key Identifier

FBCA's Forward Certs



PCA 1's Forward Certs



Phase I - Lessons Learned - Authority Key Identifier

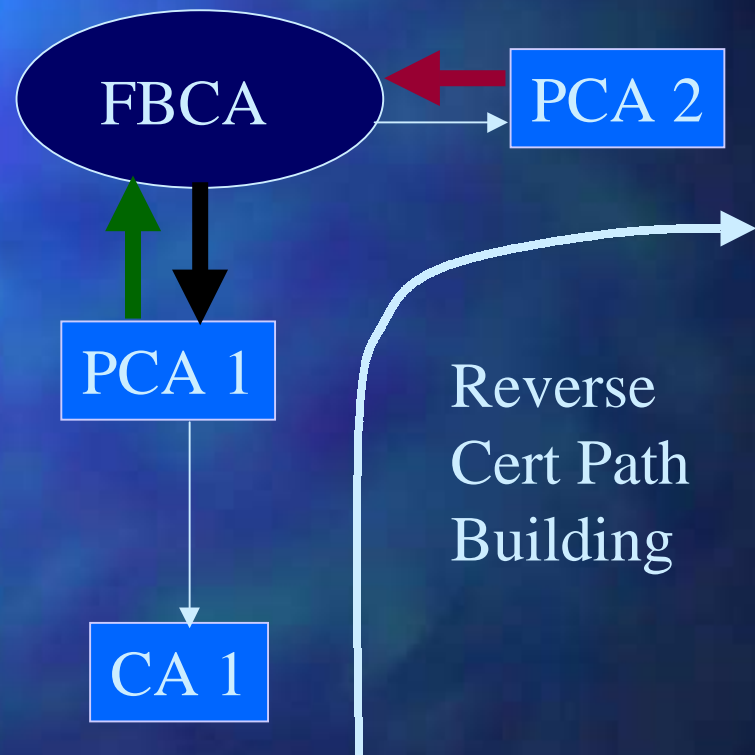
FBCA's Forward Certs

Subject Name: FBCA
Issuer Name: PCA1
Ser # 002
Subj Key ID:
Issuer: PCA1
Ser #: 002
Auth Key ID:
Issuer: PCA1
Ser #: 000

Subject Name: FBCA
Issuer Name: PCA2
Ser #: 010
Subj Key ID:
Issuer: PCA2
Ser #: 000
Auth Key ID:
Issuer: PCA2
Ser #: 000

Subject Name: PCA 1
Issuer Name: FBCA
Ser # 100
Subj Key ID:
Issuer: PCA1
Ser #: 001
Auth Key ID:
Issuer: PCA1
Ser #: 002

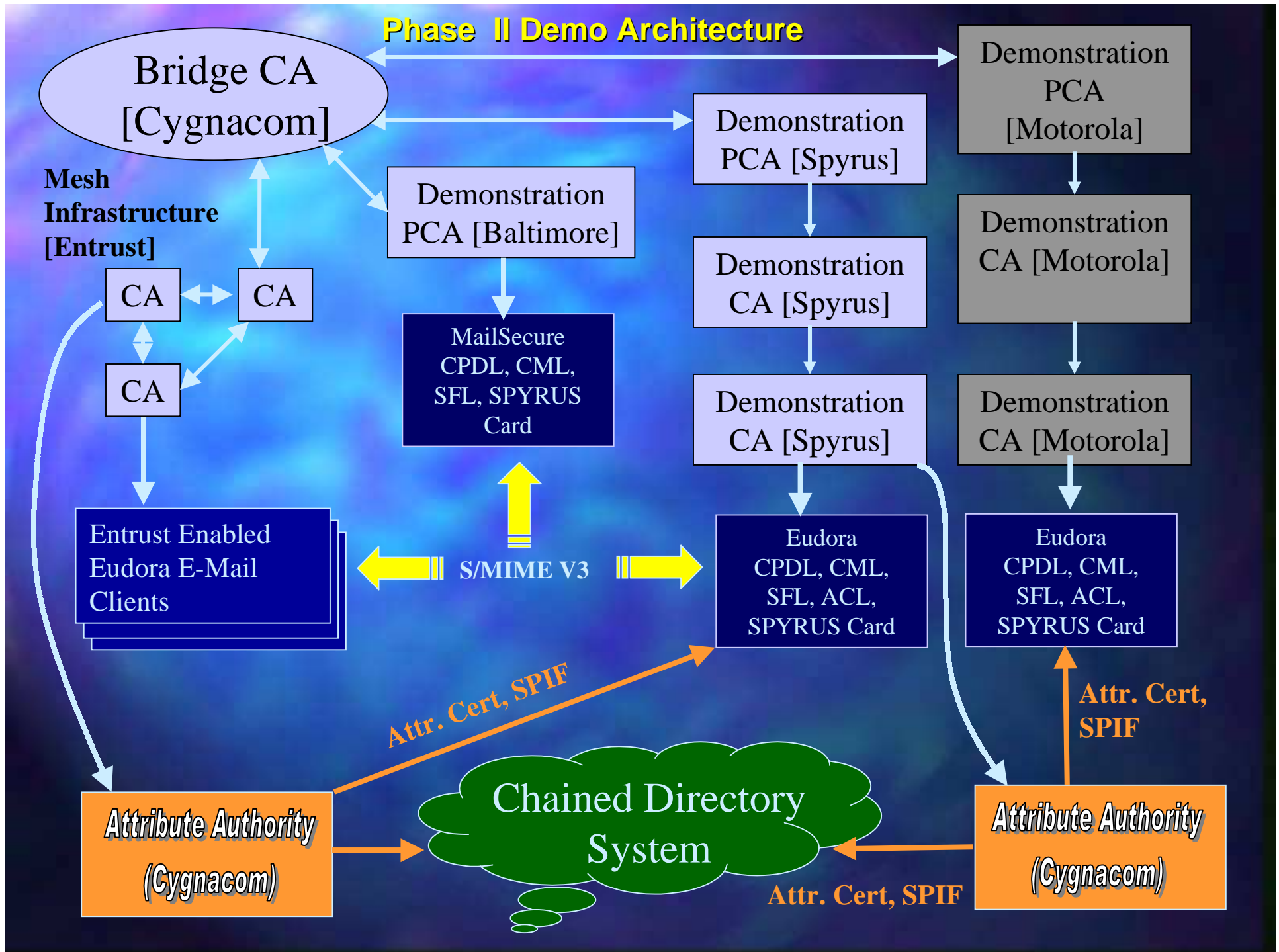
PCA 1's Forward Certs



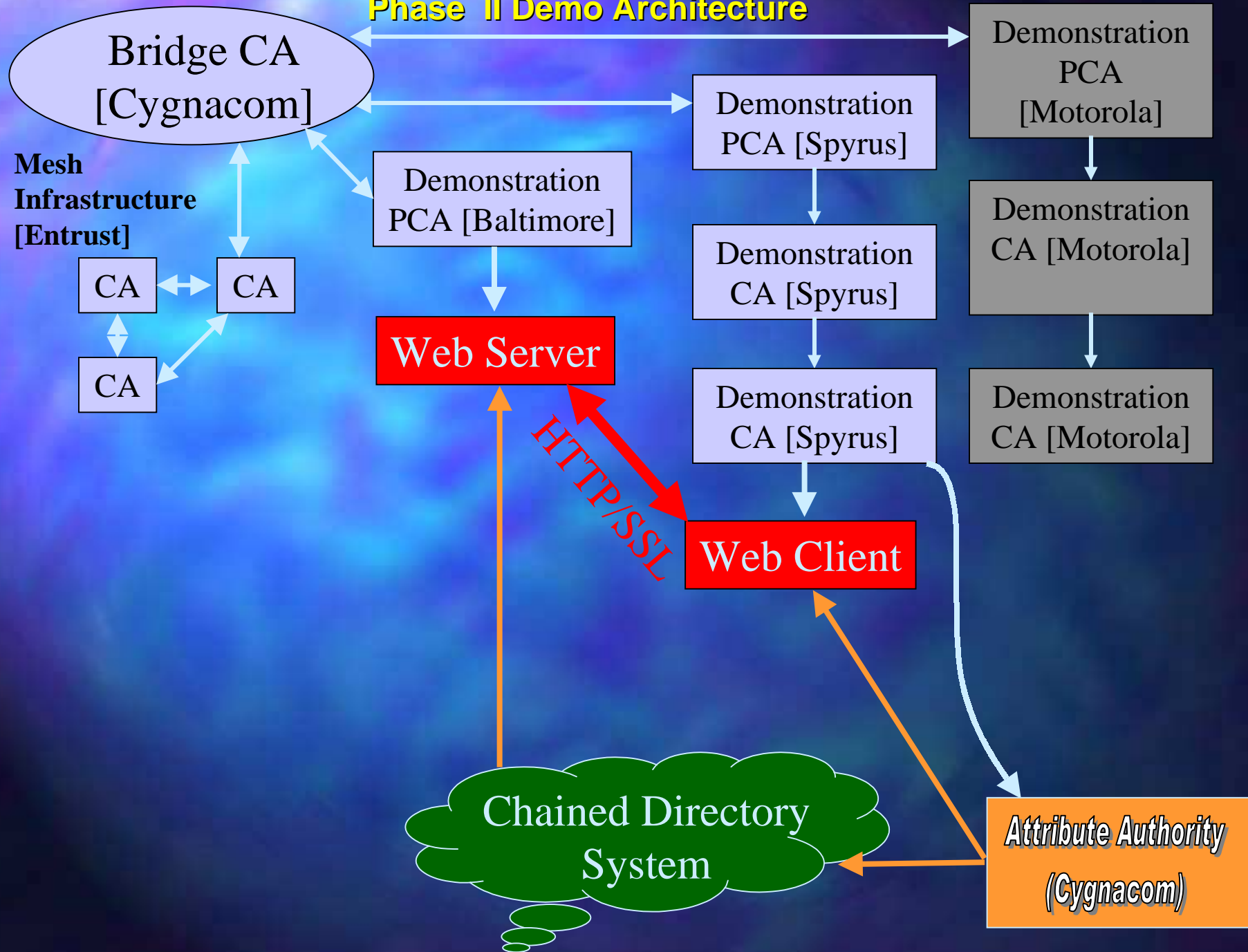
Phase II - Goals

- Build on Phase I
- Add encryption (Ephemeral/Static DH, 3DES)
- Add key recovery
- Add Attribute Certificate based access control - Based on SDN.801 (Security Policy Agility)
- Signature Algorithm Agility (RSA/DSS/SHA1/MD5)
- Client Certificate Policy Processing
- Name Constraint Processing
- Add Baltimore Technologies CA, Client
- Add web application with BCA authentication, Attribute Certificate access control

Phase II Demo Architecture



Phase II Demo Architecture



Summary

- Phase I a success!
- Integration with Federal BCA relatively simple
- CA product interoperation requires work, but can be done - Not the hardest part of the problem
- Directory product interoperation difficulty varies greatly - but can be done - and very effectively
- Clients can be enabled with freely available software
- Phase II to exercise every feature required for fully functional Federal PKI